

CLAIMS:

1 1. A Bluetooth based security system, comprising:
2 a secured device (SD) equipped with Bluetooth (BT) technology;
3 a plurality of Bluetooth Access Points (BTAPs) located at designated points to establish a
4 BT link with said secured device (SD); and
5 a security server (SS) connected to all BTAPs and arranged to provide access control and
6 security services for said secured device (SD),

 wherein said security server (SS) obtains attribute information of said secured device
(SD), including an unique device identification (ID) and a last known location of said secured
device (SD), activates a lock with said secured device (SD), and sends location information of a
designated BTAP and an unlock code to said secured device (SD), via said designated BTAP.

2 2. The Bluetooth based security system as claimed in claim 1, wherein said attribute
3 information of said secured device (SD) is captured by the BTAPs and registered in a database of
said security server (SS).

1 3. The Bluetooth based security system as claimed in claim 1, wherein said lock is
2 activated between said secured device (SD) and said security server (SS), via said designated
3 BTAP, upon a request from said secured device (SD) or upon an expiration of a pre-defined
4 timeout value of said security server (SS).

1 4. The Bluetooth based security system as claimed in claim 1, wherein said security
2 server obtains the unique device identification (ID) from said secured device (SD) and the last
3 known location of said secured device (SD) from the last BTAP that said secured device (SD)
4 connected with.

1 5. The Bluetooth based security system as claimed in claim 1, wherein said security
2 server (SS) is connected to the Internet or other networks to provide remote monitoring and
3 tracking of said secured device (SD).

1 6. The Bluetooth based security system as claimed in claim 1, wherein said security
2 server (SS) is configured to notify the owner of said secured device (SD) if said secured device
3 (SD) is lost through unauthorized BT disconnection.

1 7. The Bluetooth based security system as claimed in claim 1, wherein said secured
2 device (SD) sends the unlock code back to said security server (SS) to disengage the lock,
3 thereby making said secured device (SD) free to roam.

1 8. The Bluetooth based security system as claimed in claim 1, wherein said security
2 server (SS) comprises:
3 a database arranged to store attribute information of said secured device (SD), including

4 the unique device identification (ID) and the last known location of said secured device (SD);
5 a processor configured with a security control software to provide ad-hoc security
6 services, including remote monitoring and tracking of said secured device (SD); and
7 an I/O subsystem arranged to install the security control software and change system
8 settings and configurations, and to establish connections with the Internet or other networks to
9 provide security services, including remote monitoring and tracking of said secured device (SD).

1 9. The Bluetooth based security system as claimed in claim 8, wherein said secured
2 device (SD) comprises:
3 a processor;
4 a host chipset connected to the processor;
5 a memory connected to the host chipset and arranged to contain an operating system (OS)
6 and a security control software for activating/deactivating a lock with the BTAPs; and
7 a Bluetooth transceiver connected to the host chipset and arranged to contain an antenna
8 complex for establishing communication with any of the BTAPs for security services.

1 10. The Bluetooth based security system as claimed in claim 9, wherein said secured
2 device (SD) further comprises:
3 a Global Positioning System (GPS) receiver connected to the host chipset and arranged to
4 contain an antenna complex for providing radio positioning and navigation needs, including
5 receiving location information of said secured device (SD) relative to the BTAPs and

6 determining a change in distance between said secured device (SD) and said designated BTAP.

1 11. The Bluetooth based security system as claimed in claim 9, wherein said
2 Bluetooth transceiver contains the unique device identification (ID) of said secured device (SD)
3 for identification and communication with any one of the BTAPs strategically located at
4 designated points where said secured device (SD) is most likely secured temporarily or
5 permanently.

1 12. The Bluetooth based security system as claimed in claim 11, wherein said
2 Bluetooth transceiver comprises:
3 a radio-frequency (RF) unit arranged to transmit/receive radio waves to/from any one of
4 the BTAPs, via the antenna complex;
5 a baseband unit arranged to establish link set-up (control) and support for link
6 management between said secured device (SD) and the BTAPs, including user authentication
7 and link authorization; and
8 a Bluetooth data processor arranged to process sample Bluetooth data, including the
9 location of the last BTAP that said secured device (SD) connected with.

1 13. The Bluetooth based security system as claimed in claim 10, wherein said GPS
2 receiver comprises:

3 a radio-frequency (RF) unit arranged to receive GPS data from a plurality of GPS

4 satellites, via the antenna complex;
5 a baseband unit arranged to sample GPS data; and
6 a GPS data processor arranged to process sample GPS data relating to the location of said
7 secured device (SD) relative to the BTAPs and determine a change in distance between said
8 secured device (SD) and said designated BTAP.

1 14. The Bluetooth based security system as claimed in claim 1, wherein, when said
2 lock is activated between said security server (SS) and said secured device (SD), via said
3 designated BTAP, said security server (SS) transmits the location information (X, Y, Z
4 coordinates) of said designated BTAP and the unlock code to said secured device (SD) for future
5 use, and then said secured device (SD) transmits the unique device ID of said secured device
6 (SD) and the last know location (X, Y, Z coordinates) of said secured device (SD) back to said
7 security server (SS), via said designated BTAP through the BT link.

1 15. The Bluetooth based security system as claimed in claim 14, wherein said
2 security server (SS) creates log entry in its database, stores the unique device ID of said secured
3 device (SD), the last known location (X, Y, Z coordinates) of said secured device, the time, and
4 the unlock code.

1 16. The Bluetooth based security system as claimed in claim 15, wherein, if there is
2 an occurrence of an unauthorized breach event during the time when the lock between said

3 security server (SS) and said secured device (SD) is maintained, said security server (SS)
4 operates in a search and arrest mode to notify an appropriate personnel along with the last known
5 position of said secured device (SD) and initiate a network wide (or Internet wide) search and
6 arrest request for said secured device (SD).

1 17. The Bluetooth based security system as claimed in claim 16, wherein said lock is
2 deactivated if the user at said secured device (SD) input the unlock code, and the user supplied
3 unlock code matches the stored unlock code.

4 18. A method of providing security services for a secured device equipped with
5 Bluetooth, comprising:
6

7 installing a plurality of Bluetooth Access Points (BTAPs) at designated points to
8 establish a BT link with said secured device (SD);
9

10 connecting a security server (SS) to all BTAPs to provide access control and security
11 services for said secured device (SD); and

when said secured device (SD) establishes a BT link with a designated BTAP, enabling
said security server (SS) to obtain attribute information of said secured device (SD), including an
unique device identification (ID) and a last known location of said secured device (SD), activate
a lock with said secured device (SD), and send location information of a designated BTAP and
an unlock code to said secured device (SD), via said designated BTAP.

1 19. The method as claimed in claim 18, wherein said attribute information of said
2 secured device (SD) is captured by the BTAPs and registered in a database of said security
3 server (SS).

1 20. The method as claimed in claim 18, wherein said lock is activated between said
2 secured device (SD) and said security server (SS), via said designated BTAP, upon a request
3 from said secured device (SD) or upon an expiration of a pre-defined timeout value of said
 security server (SS).

1 21. The method as claimed in claim 18, wherein said security server obtains the
2 unique device identification (ID) from said secured device (SD) and the last known location of
3 said secured device (SD) from the last BTAP that said secured device (SD) connected with.

1 22. The method as claimed in claim 18, wherein said security server (SS) is
2 connected to the Internet or other networks to provide remote monitoring and tracking of said
3 secured device (SD).

1 23. The method as claimed in claim 18, wherein said security server (SS) is
2 configured to notify the owner of said secured device (SD) if said secured device (SD) is lost
3 through unauthorized BT disconnection.

1 24. The method as claimed in claim 18, wherein said secured device (SD) sends the
2 unlock code back to said security server (SS) to disengage the lock, thereby making said secured
3 device (SD) free to roam.

1 25. The method as claimed in claim 18, wherein, when said lock is activated between
2 said security server (SS) and said secured device (SD), via said designated BTAP, said security
3 server (SS) transmits the location information (X, Y, Z coordinates) of said designated BTAP
4 and the unlock code to said secured device (SD) for future use, and then said secured device
5 (SD) transmits the unique device ID of said secured device (SD) and the last know location (X,
6 Y, Z coordinates) of said secured device (SD) back to said security server (SS), via said
7 designated BTAP through the BT link.

1 26. The method as claimed in claim 18, wherein said security server (SS) creates log
2 entry in its database, stores the unique device ID of said secured device (SD), the last known
3 location (X, Y, Z coordinates) of said secured device, the time, and the unlock code.

1 27. The method as claimed in claim 18, wherein, if there is an occurrence of an
2 unauthorized breach event during the time when the lock between said security server (SS) and
3 said secured device (SD) is maintained, said security server (SS) operates in a search and arrest
4 mode to notify an appropriate personnel along with the last known position of said secured
5 device (SD) and initiate a network wide (or Internet wide) search and arrest request for said

6 secured device (SD).

1 28. The method as claimed in claim 18, wherein said lock is deactivated if the user at
2 said secured device (SD) input the unlock code, and the user supplied unlock code matches the
3 stored unlock code.

1 29. A computer readable medium having stored thereon a plurality of instructions
which, when executed by a processor of a security server (SS) providing security services for a
secured device (SD) equipped with Bluetooth via a plurality of Bluetooth Access Points
(BTAPs), cause the processor to perform:

5 establishing a link with said secured device (SD) via a designated BTAP, when said
6 secured device (SD) is in proximity of said designated BTAP;

7 obtaining attribute information of said secured device (SD), including an unique device
8 identification (ID) and a last known location of said secured device (SD);

9 activating a lock with said secured device (SD), via said designated BTAP, upon a
10 request from said secured device (SD) or upon an expiration of a pre-defined timeout value;

11 sending location information of said designated BTAP and an unlock code to said
12 secured device (SD), via said designated BTAP.

1 30. The computer readable medium as claimed in claim 29, further enabling, if there
2 is an occurrence of an unauthorized breach event during the time when the lock between said

3 security server (SS) and said secured device (SD) is maintained, operation in a search and arrest
4 mode to notify an appropriate personnel along with the last known position of said secured
5 device (SD) and initiate a network wide (or Internet wide) search and arrest request for said
6 secured device (SD).

TOP SECRET